AIR FORCE RESEARCH LABORATORY (AFRL)

Enterprise RDT&E IT Support (ERITS)

Performance Work Statement (PWS)
ID05190045

Table of Contents

Document Change Log

Date of Change	What was Changed	Reason for Change

1.0 Background

Air Force Research Laboratory (AFRL)

The Air Force Research Laboratory (AFRL) is the primary research and development organization for the U.S. Air Force. AFRL consists of nine Technology Directorates (TDs) and a headquarters organization with over 11,000 members including over 6,000 scientists and engineers (S&Es). AFRL is headquartered at Wright Patterson Air Force Base (WP AFB) (AFRL HQ, Sensors Directorate, Materials Directorate, Aerospace Vehicles Directorate, and the 711th Human Performance Wing) with remote organizations at Arlington, Virginia (Air Force Office of Scientific Research); Rome, NY (Information Directorate); Eglin AFB, FL (Weapons Directorate); Kirtland AFB, NM (Space Vehicles Directorate and Directed Energy Directorate); Edwards AFB, CA (Aerospace Vehicles Directorate); and Maui, HI (Directed Energy Directorate).

Research Collaboration and Computing Directorate (RC)

The Research Collaboration and Computing Directorate (RC) provides enterprise Information Technology (IT) capabilities to AFRL. RC has four divisions: Business IT (RCB); High Performance Computing (RCM); Enterprise IT Strategy and Cyber Security (RCC); and the Operations division (RCO). RC staff are spread across several buildings at WP AFB, OH (buildings 676, 15, and 16).

Research Development Test and Evaluation (RDT&E) Environments

AFRL has over 13,000 research, development, test, and evaluation (RDT&E) IT systems using a diverse set of operating systems including Microsoft Windows 10 (roughly 45%), Apple Mac OSX (roughly 10%), and various Open Source Linux distributions (roughly 45%) (Red Hat Enterprise Linux, CentOS, Scientific Linux, Fedora, Ubuntu, and OpenSUSE, etc.). These systems are spread across several networks depending on requirements. The uNclassified Internet Protocol Routing NETwork (NIPRnet) or Air Force NETwork (AFNET) is the Air Force business and operations network. AFRL has moved the majority of research IT systems off of AFNET because of strict security constraints that impede conducting research. The Defense Research and Engineering Network (DREN) is a high speed (100Gbps backbone), low latency network dedicated to research and engineering. Most of AFRL's research IT systems that require external network access (Internet) are connected to enclaves connected to DREN.

Depending on requirements, some systems may be separated off onto isolated/segregated or stand-alone networks that maximize flexibility but greatly limits collaboration between labs and sites. AFRL's research IT environment also spans Unclassified, Collateral Secret, and Top Secret and above networks.

Enterprise RDT&E Services

Enterprise Laboratory Services Zone (ELSZ)

The AFRL RDT&E ELSZ is a research collaboration and information sharing system intended to meet the unique needs of AFRL's S&Es. It is intended to support collaboration between AFRL sites as well as between AFRL S&Es and their external partners (academics, contractors, other government agencies, and other DoD services). It is not intended to duplicate other collaborative services already available through other Air Force or DoD collaboration systems (MS Sharepoint, milSuite, etc.).

The ELSZ environment currently consists of three operating environments (the Unclassified ELSZ DREN Extranet; the Unclassified ELSZ Isolated Intranet; and the Classified (Collateral Secret) Isolated Intranet) and a fourth environment being constructed (an experimental and prototype virtual machine hosting sandbox).

The current ELSZ environments are based on virtualized servers running on top of a type 1 hypervisor on blade servers connecting to an iSCSI (Internet Small Computer System Interface) based Storage Area Network (SAN) via multiple 10Gbps Ethernet links. The overall environment has a 10Gbps Ethernet link to the DREN. The virtual servers providing the user and infrastructure capabilities are typically running either Scientific Linux or CentOS Linux – migrating to just CentOS Linux. There are also a handful of Microsoft Windows based servers for Windows Update Services and Active Directory (AD) authentication services. The user and infrastructure services are provided by predominantly Open Source Software applications (examples include but are not limited to: Apache and NGINX web servers, PHP and Ruby web applications (NextCloud, TikiWiki, MediaWiki, osTicket, etc.), MySQL/MariaDB database servers and SFTP) and some commercial software (an example is GitLab Enterprise).

The entire ELSZ system is housed in the building 676 data center at WP AFB in Dayton, Ohio.

Enterprise RDT&E Network Operations Center (NOC)

The complexity of the distributed AFRL RDT&E network environment has grown to the point where a centralized NOC has become necessary. All of the infrastructure support capabilities currently hosted under the ELSZ will be logically migrated to the Enterprise RDT&E NOC. The enterprise RDT&E NOC will provide centralized support services and monitoring and cyber

security infrastructure services to all of AFRL's RDT&E network enclaves across DREN and isolated environments and at multiple classification levels (unclassified and collateral Secret to start). The infrastructure for the enterprise RDT&E NOC will reside in building 676 at WP AFB, Ohio.

2.0 Enterprise Laboratory Services Zone (ELSZ) Support CLIN 0001

2.1 Scope

The contractor shall perform the following task areas across all of the current and future environments and capabilities described in Appendix A, Section A.1 (AFRL RDT&E ELSZ Environment Breadth and Complexity). The AFRL RDT&E ELSZ system is focused on user capabilities supporting research collaboration and information sharing.

2.2 Task Areas

2.2.1 Research / Investigation

The contractor shall research and investigate new research collaboration and information sharing capabilities and new ELSZ zones as identified by the ELSZ Program Manager. The contractor shall provide results of their research to the ELSZ Program Manager.

2.2.2 Prototyping

The contractor shall prototype new capabilities as identified by the ELSZ Program Manager. New capabilities shall be developed in an environment with access restrictions defined by the ELSZ Program Manager.

2.2.3 Testing

The contractor shall test capabilities as requested by the ELSZ Program Manager. Test virtual systems shall be developed in an environment with access restrictions defined by the ELSZ Program Manager.

2.2.4 Implementation

The contractor shall implement ELSZ capabilities on virtualized and or containerized systems built using automated processes (Puppet/Foreman). All code implementing system configuration changes or any manual changes shall be managed using a configuration

management system (for example: git-based repositories) or alternative defined by the ELSZ Program Manager.

The contractor shall construct a virtualized and or containerized (Docker, OpenStack, Kubernetes, etc.) service infrastructure for the new zones as decided by the ELSZ Program Manager. New zones would be implemented based on the configuration of existing zones. All application and user data and databases shall be stored on the network storage and not within the virtual machine disk image unless pre-approved by the Program Manager. The contractor shall configure the servers into logically or physically segregated pools so that access to Virtual Machines can be restricted to just contractor system admin staff or open to all ELSZ users or open to contractor system admin staff and select test users.

2.2.5 Database Management

The contractor shall implement, configure, harden, operate, and optimize a variety of database servers to include at least MySQL, MariaDB, and PostgreSQL to support web based user applications.

2.2.6 Operations

Once the virtualization/containerization foundation, supporting infrastructure capabilities, and collaborative capabilities are in place, operational, and security hardened – the contractor shall maintain these capabilities in compliance with Federal, DoD and AF IT and security requirements listed in Appendix B.

The contractor shall perform weekly back-ups (full back-up each weekend with incremental back-ups nightly) of user data and system images. The contractor shall deliver unclassified back-up media (portable USB hard drives, backup tapes, etc.) to the ELSZ program management team for off-site storage (outside of the WPAFB building 676 data center) on a quarterly basis.

The contractor shall create and maintain a software license repository in WPAFB, Area B, Building 16, Room 110. A copy of all software, software license documentation, and software license keys used in the environment shall be placed in the ELSZ project off-site storage container (or other government directed location). This software could be Open Source Software, government purchased and provided commercial software, or contractor purchased software.

All activities shall be carried out in full compliance with relevant Federal, DoD, AF, AFMC, Base, and Organizational regulations, instructions, and procedures listed in Appendix B. The contractor shall be responsible for assessing and adapting operations to comply with changes

in official Government policy in these areas when notified by the Government team that a relavent policy has changed that could affect work done on this contract.

The contractor staff will enter and track all user support issues and non-helpdesk/non-repeating work in a web-based helpdesk ticket and issue tracking system that is part of the overall ELSZ system. Contractor use of the Government identified system is mandatory. This includes all work done on the systems whether it is a user support issue or an internal issue.

The ELSZ system has been described as a non-mission critical system. The system description and system security authorization package describe that uptime will be best effort during normal business hours. Scheduled downtime due to system or application patching or restarting shall be minimized during normal duty hours and coordinated with the ELSZ Program Manager. Unscheduled downtime shall be reported to the ELSZ Program Manager as soon as possible. Classified data spillage incidents, major hardware failures, or other events such as power outages or weather related issues could cause significant delays in a return to normal operational status. A return to operational status will be best effort during normal duty hours when facilities are accessible.

The ELSZ operations shall be manned by the contractor, at a minimum, from 8am to 5pm, Eastern Daylight Time (EDT), Monday through Friday except Federal holidays.

2.2.7 Maintenance

The contractor shall maintain all ELSZ components and systems. Significant patches or updates shall not be done on live production servers. Servers shall be cloned and the system clone moved to the segregated test area. Patches or updates shall be applied to the system clone and then tested. If there are no problems then the patched or updated clone shall replace the current production server.

All physical and virtual server Secure Shell (SSH) based access shall be via CAC certificate or SSH-key based authentication. All SSH processes shall be configured to deny username-password authentication, unless absolutely required as determined by the Government Program Manger, on a system by system basis, for all physical and virtual systems across all support environments. All formal systems administrators' SSH keys shall be replicated to all physical and virtual systems across all support environments.

2.2.8 System and Capability Monitoring

The contractor shall implement capabilities necessary to automate the collection and display of systems, capability usage, and reliability metrics data on web-based dashboards. These dashboards shall be accessible to anyone with an account in the environment.

2.2.9 Cyber Security

The contractor shall ensure that all contractor staff servicing the organization are made aware of their duties, restrictions, procedures and regulations relating to information security. Contractor-provided Information Assurance (IA) services shall include, but are not limited to:

- Implementing and tracking compliance with network security directives
- Conducting weekly scheduled vulnerability scans using at least ACAS, and resolving identified issues
- Conducting ad hoc vulnerability scans using ACAS as necessary
- Tracking and resolving malicious logic incidents
- Handling account requests to include creating the accounts, password resets, updates to accounts, ect
- Resolution of classified spillage incidents. A spillage incident could be identified by either Government or Contractor personnel. The Contractor would be in charge of notifying the Cyber Security Office who will inform the Contractor the steps to resolve the issue

All physical and virtual servers shall be security hardened according to the relevant (Linux, MS Windows, Apache Web Server, Database Server, etc.) DISA Security Technical Implementation Guides (STIGs) or as documented in the system security authorization package (A&A). All approved deviations from the STIG configurations shall be documented in a Plan of Actions and Milestones (POA&M) as part of the AFRL Enterprise RDT&E environment Risk Management Framework (RMF) A&A package.

All physical and virtual servers shall have all Air Force designated Category 1, critical, and high vulnerabilities corrected or mitigated within one week of detection and identification. Air Force designated Category 2, 3, and medium vulnerabilities shall also be corrected or mitigated within 30 days. Air Force designated low vulnerabilities shall be corrected or mitigated within 60 days. DoD/AF will determine the level of vulnerability. The contractor shall create POA&M entries for any vulnerability that cannot be corrected, to document mitigation measures.

The contractor shall provide STIG compliance reports and resolved vulnerability scan reports to the Information System Security Manager (ISSM) for inclusion in the (A&A).

2.2.10 Help Desk Operations

The ELSZ HelpDesk shall be operated and manned by the contractor during normal AFRL business hours (8am to 5pm), Eastern Standard Time (EST), Monday through Friday excluding Federal Holidays.

The contractor shall provide user support (helpdesk operations) to users (currently 1600 total users with 600 regularly active users but growing rapidly) of the ELSZ systems (currently the Unclassified DREN Extranet, Unclassified Isolated Intranet, and the Classified Collateral Secret Isolated Intranet). Support shall include, but is not limited to: creating accounts; assisting users in resetting or updating their passwords or other authentication credentials; and assisting users with using any of the user facing services of the ELSZ systems. The contractor shall also perform network and system troubleshooting to determine root causes of any user issues or problems. The helpdesk administrator(s) shall also assist the primary systems administrators or other contract functionals when not performing helpdesk functions.

The Contractor staff shall enter and track all user support issues in a web-based helpdesk ticket tracking system that is part of the overall ELSZ system.

The contractor shall provide an initial response to helpdesk queries within 4 business hours. Requests received at the end of the business day shall be responded to the morning of the next business day. The contractor shall create user accounts within 1 business day of receiving the completed and approved request form. The contractor shall create new project, working group, community of interest, etc. sites within 5 business days of receiving an ELSZ program manager approved, request. The definitions of helpdesk ticket levels shall be as follows: A level 1 helpdesk ticket is a request that could reasonably be completed within 3 business days; A level 2 helpdesk ticket is a request that could reasonably be completed within 2 business weeks and a level 3 ticket is one that could reasonably be expected to take longer than 2 weeks to complete. The contractor shall collect and report on response time metrics in the monthly status report.

2.2.11 Training

The contractor shall learn and become proficient in the configuration and use of the ELSZ collaboration applications. The contractor shall develop and keep current wiki-based and other online training for the ELSZ and Network Operations Center (NOC) capabilities. The contractor shall conduct in-person/on-site and Video Teleconference (VTC) based training sessions with end users. The contractor shall assist users with the configuration of ELSZ collaboration applications to meet their project or working group requirements or use case.

2.2.12 Software/Web Application Development or Modification

The contractor shall modify existing ELSZ open source web applications, unless an alternative method is pre-approved by the Program Manager, to allow CAC/PKI-cert only authentication. These modifications shall be contributed to the original open source application projects, if approved by the Government Program Manager, to ensure that future versions of these Open Source Software applications include this functionality.

The contractor may also be required to develop, modify, or configure existing software applications (could be Open Source Software applications or commercial applications purchased and provided by the Government) to support system usage and reliability metrics dashboarding and monitoring. All code developed or modifications developed for open source software applications under this contract shall be delivered with unlimited rights.

2.2.13 Documentation Support

The contractor shall support maintenance of the A&A by creating and maintaining content for the documentation, drawings, etc., as necessary.

The contractor shall maintain continuity documentation of all processes, procedures, and system & application configurations used in the operations and maintenance of the environment.

The contractor shall develop user instructions and other documentation to inform users on how to utilize the ELSZ capabilities. This documentation shall be maintained in the ELSZ Wiki and Frequently Asked Questions (FAQ).

3.0 AFRL Enterprise RDT&E NOC Support CLIN 0002

3.1 Scope

The contractor shall perform the following task areas across all of the current and future environments and capabilities described in Appendix A, Section A.2 (AFRL Enterprise RDT&E NOC Environment Breadth and Complexity). While the AFRL RDT&E ELSZ capability focuses on end user (scientist and engineer) facing capabilities – the AFRL Enterprise RDT&E NOC focuses on infrastructure support and network management capabilities supporting the entire AFRL enterprise RDT&E IT environment.

3.2 Task Areas

3.2.1 Research / Investigation

The contractor shall research and investigate new capabilities as identified by the Enterprise RDT&E NOC Program Manager. Results of the research conducted by the contractor shall be delivered to the NOC Program Manager.

3.2.2 Prototyping

The contractor shall prototype new capabilities as identified by the Enterprise RDT&E NOC Program Manager. New capabilities shall be developed in an environment with access restrictions defined by the NOC Program Manager.

3.2.3 Testing

The contractor shall test capabilities as identified by the ELSZ Program Manager. Test virtual systems shall be developed in an environment with access restrictions defined by the NOC Program Manager.

3.2.4 Implementation

The contractor shall implement NOC capabilities on virtualized and or containerized (Docker, OpenStack, Kubernettes, etc.) systems built using automated processes (currently utilizing Puppet/Foreman) as decided by the NOC Program Manager. All code implementing system configuration changes or any manual changes shall be managed using a configuration management system (currently git-based repositories) unless pre-approved by the NOC Program Manager.

The contractor shall implement a virtualized and or containerized service infrastructure. All data and databases shall be stored on the network storage and not within the virtual machine disk image unless pre-approved by the NOC Program Manager. The contractor shall configure the servers into logically or physically segregated pools so that access to Virtual Machines can be restricted to just NOC staff or open to all RDT&E users.

3.2.5 Operations

Once the virtualization/containerization foundation, supporting infrastructure capabilities, and collaborative capabilities are in place, operational, and security hardened – the contractor shall maintain these capabilities in compliance with Federal, DoD and AF security requirements listed in Appendix B.

The contractor shall perform weekly back-ups (full back-up each weekend with incremental back-ups nightly) of critical system data and system images. The contractor shall deliver

unclassified back-up media (portable USB hard drives and backup tapes) to the NOC program management team for off-site storage (outside of the WPAFB building 676 data center) on a quarterly basis.

A copy of all software, software license documentation, and software license keys used in the environment shall be placed in the NOC project off-site storage container in Area B, building 16, room 110, WP AFB (or other government directed location).

All activities shall be carried out in full compliance with relevant Federal, DoD, AF, AFMC, Base, and Organizational regulations, instructions, and procedures listed in Appendix B. The contractor shall be responsible for assessing and adapting operations to comply with changes in official Government policy in these areas once a relevant policy or instruction change has been identified by the Government.

The NOC operations staff will enter and track all user support issues and non-helpdesk/non-repeating work in a web-based helpdesk ticket and issue tracking system that is part of the overall NOC system.

The NOC system has been described as a non-mission critical system. The system description and system security authorization package describe that uptime will be best effort during normal business hours. Downtime due to system or application patching or restarting should be minimized during normal duty hours. Classified data spillage incidents, major hardware failures, or other events such as power outages or weather related issues could cause significant delays in a return to normal operational status. A return to operational status will be best effort during normal duty hours when facilities are accessible.

The NOC operations shall be manned by contractor staff, at a minimum, from 8am to 5pm, Eastern Daylight Time (EDT), Monday through Friday except Federal holidays.

3.2.6 Maintenance

The contractor shall maintain all ELSZ components and systems. Significant patches or updates shall not be done on live production servers. Servers shall be cloned and the system clone moved to the segregated test area. Patches or updates will be applied to the system clone and then tested. If there are no problems then the patched or updated clone shall replace the current production server.

All physical and virtual server Secure Shell (SSH) based access shall be via CAC certificate or SSH-key based authentication. All SSH processes shall be configured to deny username-password authentication, unless absolutely required on a system by system basis, for all physical and virtual systems across all support environments. All formal systems

administrators' SSH keys shall be replicated to all physical and virtual systems across all support environments.

3.2.7 System and Capability Monitoring

The contractor shall implement capabilities necessary to automate the collection and display of system and capability usage and reliability metrics data on web-based dashboards. These dashboards shall be accessible to anyone with an account in the environment.

3.2.8 Cyber Security

The contractor shall ensure that all members servicing the organization are made aware of their duties, restrictions, procedures and regulations relating to information security. Contractor-provided cyber security services shall include, but not be limited to:

- Implementing and tracking compliance with network security directives
- Overseeing and following up on regularly scheduled vulnerability scans
- Tracking and resolving malicious logic incidents
- Handling account requests
- Resolution of classified spillage incidents

All physical and virtual servers shall be security hardened according to the relevant (Linux, MS Windows, Apache Web Server, Database Server, etc.) DISA STIGs or as documented in the A&A. All approved deviations from the STIG configurations shall be documented in a POA&M as part of the AFRL RMF A&A package.

All physical and virtual servers shall have all Air Force designated Category 1, critical, and high vulnerabilities corrected or mitigated as feasible within one week of detection and identification. Air Force designated Category 2, 3, and medium vulnerabilities shall also be corrected or mitigated as feasible within 30 days. Air Force designated low vulnerabilities shall be corrected or mitigated within 60 days. DoD/AF will determine the level of vulnerability. POA&Ms shall be created for any vulnerability that cannot be corrected, to document mitigation measures.

The contractor shall provide STIG compliance reports and resolved vulnerability scan reports to the Information System Security Manager (ISSM) for inclusion in the system security authorization package (A&A).

3.2.9 Network Management

The contractor shall manage the enterprise RDT&E core network infrastructure to the External Router and External Firewall that are connected to the DREN Point of Presence at WP AFB. The contractor shall build and manage the firewall rules to control traffic to the enterprise environments. Since the enterprise RDT&E core network infrastructure is entirely based on Cisco brand equipment, this work will require a minimum of a Cisco Certified Network Administrator.

The contractor shall install, configure, and manage all internal network devices in each service zone (Unclassified DREN, Unclassified Isolated, Collateral Secret Isolated, etc.) to include but not be limited to top of rack switches, blade chassis network switches, storage switches, VPN appliances, and TACLANE encryptors.

AFRL Unclassified RDT&E Isolated Network Interconnects Management: The contractor shall deploy, install, configure, and manage the VPN/firewall appliances to build the AFRL unclassified RDT&E wide-area isolated network. The contractor shall pre-configure the appliances as much as possible and ship them to identified AFRL sites. The contractor shall coordinate schedules and procedures with those AFRL sites to deploy and configure the VPN end points to join them into the wide area isolated network. The contractor shall utilize a centralized management console to maintain the network VPN interconnects and configure firewall rules to control traffic on the wide-area isolated network (what traffic is allowed to the ELSZ Isolated Intranet and what traffic is allowed between the interconnected laboratory networks). Some travel may be required to visit connecting sites to assist with implementation and configuration of the VPN appliances.

AFRL Classified RDT&E Isolated Network Interconnects Management: The contractor shall deploy, install, configure, and manage the TACLANE encryptors to build the AFRL RDT&E classified wide-area isolated network. The contractor shall pre-configure the appliances as much as possible and ship them to identified AFRL and AFRL-partner sites. The contractor shall coordinate schedules and procedures with those sites to deploy and configure the TACLANEs to join them into the classified wide area isolated network. Some travel may be required to visit connecting sites to assist with implementation and configuration of the TACLANE appliances.

3.2.10 Remote Workstation Management

The contractor shall build, configure, install, and remotely manage standardized Linux and Microsoft Windows workstations for the interconnected isolated network environments (currently approximately 20 systems at 8 sites in phase 1, an additional 28 systems at an

additional 14 sites in phase 2, and a projected additional 20 systems at an additional 10 sites in phase 3. Additional deployment phases, systems, and sites are TBD). Systems management and configuration management of the remote systems shall be accomplished using automated configuration management tools such as Puppet and Active Directory deployed Group Policy Objects (GPOs) unless an alternate method is pre-approved by the Government Program Manager.

3.2.11 Software/Web Application Development or Modification

The contractor may also be required to develop, modify, or configure existing software applications (could be Open Source Software applications or commercial software purchased and provided by the Government) to support system usage and reliability metrics automated data collection, dashboarding, and monitoring.

3.2.12 Documentation Support

The contractor shall support maintenance of the system security authorization package by creating and maintaining content for the documentation, drawings, etc. as identified by the Government Program Manager.

The contractor shall maintain continuity documentation of all processes, procedures, and system and application configurations used in the operations and maintenance of the environment.

3.2.13 Automated Data Processing Equipment (ADPE) Custodian Function

The contractor shall support AFRL/RCC as the primary and alternate Automated Data Processing Equipment (ADPE) custodian for all accountable equipment used within the AFRL/RCC division. [The contractor shall complete Air Force equipment custodian training.]

3.2.14 COMSEC Custodian Function

The contractor shall act as COMSEC equipment custodians for the TACLANEs that are part of this network, as well as COMSEC Key Operating Account Agents (KOAAs). [The contractor shall be required to take Air Force COMSEC custodian and key management training.]

3.2.15 Classified Courier Function

The contractor shall be required to courier classified equipment and materials between buildings and potentially between WP AFB, Ohio and remote locations.

3.2.16 Information Systems Security Manager (ISSM)

The contractor shall act as the ISSM for the overall Enterprise RDT&E IT environment. The ISSM in conjunction with the Government Program Mangager shall be responsible for creating and maintaining any AFRL Risk Management Framework (RMF) system authorization and accreditation packages for the environment with a minimum of quarterly review and potentially updates. The ISSM in conjunction with the Government Program Manager shall be responsible for creating and maintaining any necessary Memorandums of Agreement (MOAs) between the Enterprise RDT&E IT environment and the using organizations. The ISSM shall periodically review all physical and cyber security measures and make recommendations on changes to the Government Program Manager.

3.2.17 Software Testing

The contractor shall verify and conduct if necessary all software and applications used in the Enterprise RDTE IT Environment are tested and formally approved by the AFRL RDT&E Authorizing Official (AO) or if not yet tested and approved the contractor shall schedule and perform the software testing. Software testing shall address three priority areas:

1. All operating systems, application or server software and web applications used in the AFRL Enterprise RDT&E IT environment, including the ELSZ and NOC environments.
2. Common client software used to access ELSZ services (some examples could include but not be limited to FileZilla and other SFTP clients and SFTP/SSHFS clients for Windows or the Git Large File Support (LFS) extension).
3. Other RDT&E software common to the AFRL RDT&E environments that has not been tested yet.

All software testing shall use an AFRL enterprise Cyber Security office approved process and results shall be submitted for AFRL enterprise-wide RDT&E approval for use. Any existing software used that has significant updates shall be re-tested and approved by the AO prior to being put in production use. Minor software updates do not require AO re-approval but should be reviewed and approved by the Enterprise RDT&E ISSM prior to implementation.

3.2.18 Remote Isolated Network Onboarding Assistance

The contractor shall support remote AFRL or AFRL partner sites with preparing their networks, troubleshooting issues, and assisting them with developing their Risk Management Framework (RMF) packages and artifacts/documentation to get approval to connect remote laboratory resources to the AFRL wide-area isolated RDT&E network environments.

3.2.19 Project and Team Management

The contractor shall provide project and team management to coordinate efforts across the AFRL Enterprise RDT&E IT Environment under this effort. These efforts shall include the following.

3.2.19.1 Contractor must utilize awarded staffing plan to create, update, and maintain a project management plan that identifies requirements, describes the planned technical approach, organizational resources, and management, to include quality controls used to meet the project performance and schedule requirements.

3.2.19.2 Contractor must provide and manage resources necessary to ensure the staff meets ongoing, schedule and performance requirements to the Government.

3.2.19.3. Contractor must provide management of contractor personnel performing tasks in this task order. The contractor must designate a principal point of contact for technical issues. The contractor must provide an employee status report containing names and associated tasks of personnel supporting the Government.

3.2.19.4. Contractor must provide a Monthly Status Report (MSR) to the COR.

3.2.19.5. Contractor must prepare documents such as briefings, bullet point papers, and meeting minutes related to status of the performance of this task order. Deliverable format must be coordinated with the Government and approved by the COR prior to submission.

3.2.19.6. Contractor must provide the name of the Contract Manager and alternate(s) in writing to the COR. The contractor must ensure all personnel assigned to this task order meet the minimum requirements specified in the PWS. The contractor must notify the COR and GSA COR in writing by email of any changes to personnel within five (5) business days after information is known.

3.2.19.7. The contractor shall identify and implement its approach for providing and ensuring quality throughout its solution to meet the requirements of the PWS via the contractor's Quality Management Plan (QMP). The QMP shall describe the application of the appropriate methodology (i.e., quality control and/or quality assurance) for accomplishing performance requirements. The QMP shall describe how the appropriate methodology integrates with the Government's requirements. The contractor shall make the QMP available to the Government for review upon request and shall obtain acceptance of the QMP by the CO as required. The contractor shall make appropriate modifications to the QMP (at no additional cost to the Government). The Government has the right to require revisions of the QMP (at no cost to the

Government) should the QMP fail to deliver the quality of the services required at any time during performance.

3.2.19.8. Contractor must submit a trip report to the COR as well as the Government person directing the travel. Trip report should include the following details: purpose, location and length of trip, travelers, and individuals contacted during trip, synopsis of all discussions, future actions identified, decisions made, or issues of concern arising during trip.

4.0 Deliverables

All deliverables must meet professional standards and comply with the requirements set forth in this PWS. All deliverables shall be submitted in electronic format as unlocked, unencrypted Portable Document Format (PDF) file with selectable text and graphics. Delivery of Microsoft Word/Microsoft Project document format versions are desired but not required. Microsoft Project 2016 or later is required if Microsoft format versions are delivered. All electronic deliveries must be anti-virus scanned before delivery to the Government.

4.1. Contractor Submission

Deliverables are to be transmitted with a cover letter, on the prime contractor's letterhead, describing the contents, electronically through GSA's web-based procurement system, as required, and to any other destination(s) as required per the Government's request. The contractor shall provide hard copy deliverables as required per the Government's request. All deliverables shall be produced using software tools/versions as approved by the Government.

4.2. Government Review

Government personnel will have 10 business days to review deliverables (to include resubmissions) and provide written acceptance/rejection. Authorized Government representatives will notify the contractor of deliverable acceptance or provide comments in writing. The contractor shall incorporate Government comments, or provide rationale for not doing so within 5 business days of receipt of comments. Government acceptance of the final deliverable will be based on resolution of Government comments or acceptance of rationale for non-inclusion. Additional changes volunteered by the contractor will be considered a resubmission of the deliverable.

4.3. Government Delays in Reviewing Deliverables or Furnishing Items

If contractor performance or submission of deliverables is contingent upon receipt of Government furnished items (data, equipment, materials, facilities, and support) or input, or upon Government review and approval of interim items or draft documents (collectively referred to as Government Performance), the Government shall specify, if not already specified within this PWS, when it will provide such items or input, or the time it will need to perform reviews or give approvals. If the Government fails to meet item, input, review, or approval deadlines, contractor performance or submission of deliverables shall automatically be extended one business day for each day of government delay. The contractor shall promptly advise the Contracting Officer of any delays in receipt of Government furnished items, input, reviews, or approvals.

4.4. The contractor shall submit the following deliverables:

Table 4-1: Deliverable Table

DEL. #	MILESTONE or DELIVERABLE	PWS REF.	COMPLETION or DELIVERY DATE
01	Back-up media	2.2.5	Quarterly
02	STIG Compliance Reports	2.2.8	As required after risk management framework is updated.
03	Project Management Plan	3.2.19	Staffing plan due concurrent with contractor quote. Creation of full PMP due within 10 days of award. A final PMP must be submitted for acceptance no later than 10 calendar days after receipt of Government review comments. PMP must include full staffing plan and must be updated and sent to the Government when any staffing changes are made.
04	QMP	3.2.19	5 business days after Government request
05	Monthly Status Report (MSR)	4.5	10th calendar day of the month following the monthly reporting period

06	Monthly Invoice	4.6	10th calendar day of the month following the monthly reporting period
07	Integrated Master Schedule	4.7	As Needed
08	Contract Transition Plan	4.8	Within 60 days of the end of the contract period of performance.
09	Non-Disclosure Agreement	9.3	Prior to assignment to contract/order
10	Trip Report(s)	9.7.	Within 10 business days following completion of each trip
11	Kick-Off Meeting	9.9	NLT 15 business days after contract/order award
12	Kick-Off Meeting Minutes	9.9	NLT 5 business days after the meeting
13	Phase-In Plan	12	Draft due with solicitation response; final due 10 business days after receipt of Government comments

4.5. Monthly Status Report

The contractor shall include the technical progress made under this contract. The contractor shall also include, at a minimum, for the initial plan, what tasks and sub-tasks need to be performed; estimates for how long each task and sub-tasks should take; anticipated start and end dates for all tasks and sub-tasks; overall projected schedule (Gantt Chart view); who is assigned to each task and percentage of their time dedicated to the task or sub-task; other resources required for each task; task interdependencies; any external dependencies including external resource dependencies; and projected capability milestones. The monthly project plan update shall include, at a minimum, progress made on each task; how many hours were actually expended vs projected and by who; any changes to the baseline schedule; description of any issues or problem areas with a recommended fix plan; and justification for any changes to the overall schedule or individual task durations. The Monthly Status Report shall not exceed 15 pages in length and be primarily focused on the highlights and significant events of the month.

4.6. Monthly Invoice

The contractor shall provide a monthly invoice, no later than the 10th calendar day of the month following the monthly reporting period, to be submitted simultaneously with the MSR. As applicable, the invoice shall include but not be limited to:

- Clear identification of all costs.

- Labor hours expended (for labor hours tasks). The labor hours expenditure information shall include the identification of the employee name, labor category, hourly labor rate, and total number of labor hours expended.
- Timecards. As required, the contractor shall provide a copy of each employee's timecard/sheet. The timesheet shall identify the contractor employee name and number of hours claimed per day.
- Travel costs.
- Supporting documentation for travel costs. Refer to PWS 5.3 for specific requirements.
- Other Direct Costs.
- Supporting documentation for other direct costs. Refer to PWS 9.7 for specific requirements.
- As required, the contractor shall comply with line item (i.e., per individual positions, different programs, program areas, etc.) invoicing requests.

4.7. Integrated Master Schedule

The ELSZ Integrated Master Schedule (IMS) shall be one integrated schedule that contains separate sections for the ELSZ Classified Intranet, DREN Extranet, and Isolated Intranet. It shall contain sufficient detail to track all significant tasks and sub-tasks across the three environments. Each delivery shall include progress made on all tasks and sub-tasks. All scheduled work elements shall be integrated into these schedules, including Subcontractor labor and purchasing schedules. The schedules shall extend to a sufficient level of detail to mitigate risk and measure performance. The Contractor shall verify a smooth transition is accomplished during the phase-out period, if required. The Contractor shall develop, track, and deliver the IMS in Microsoft Project 2010 or later to facilitate sharing with government stake holders.

4.8. Contract Transition Plan

The Contract Transition Plan shall only be provided in the event of a transition between support contractors at the end of this contract. If necessary, the Contractor shall prepare and deliver a non-proprietary Contract Transition Plan (A003) no later than 60 calendar days prior to the end of the Period of Performance (PoP) for the orderly transfer of all items related to the continued sustainment and maintenance of all components of the ELSZ. The Contract Transition Plan shall include a description of the activities and schedule required to transition the maintenance, sustainment, help desk, and technical support functions from the current Contractor(s) to the follow-on Contractor or Government agency. The plan shall include all associated trouble shooting tickets, analysis, tools, applications, COOP, procedures, etc…to help sustain and

support the system. The Contractor Transition Plan shall cover no less than a one-month period, to include assisting a follow-on Contractor through the transition process.

5.0 Service Delivery Summary (SDS)

Performance Standards, Acceptable Quality Levels (AQLs), and Incentives/Disincentives are defined in **PWS Attachment C**, the Service Delivery Summary (SDS). The SDS criteria will be used to determine if performance requirements are met.

6.0 Voluntary Protection Program (VPP)

Applicability: This section of the PWS applies to "Applicable Contractors" as defined below.

VPP Definitions:

a) Applicable contractors. A contractor whose employees worked at least 1000 hours at the site in any calendar quarter within the last 12 months and is NOT directly supervised by the applicant (installation).

b) Days Away Restricted, and or Transfer Case Incident Rate (DART). Number of recordable injuries and illness cases per 100 full-time employees resulting in days away from work, restricted work activity, and/or job transfer that a site has experienced in a given time frame.

c) Total Case Incident Rate (TCIR). Total number of recordable injuries and illness cases per 100 full-time employees that a site has experienced in a given time frame.

d) Voluntary Protection Program: The Voluntary Protection Program (VPP) promotes effective worksite-based safety and health. In the VPP, management, labor, and OSHA establish cooperative relationships at workplaces that have implemented a comprehensive safety and health management system. Approval into VPP is OSHA's official recognition of the outstanding efforts of employers and employees who have achieved exemplary occupational safety and health.

Requirements:

WP AFB is recognized under the Occupational Safety and Health Act (OSHA) VPP. VPP impacts all "applicable contractors" operating on Air Force Installations. It is the contractor's responsibility to ensure its employees and managers have a comprehensive understanding of VPP as well as full compliance with OSHA requirements. The contractor shall follow the safety

and health rules of the installation or VPP site. Detailed information on VPP is available on the OSHA website at https://www.osha.gov/dcsp/vpp/index.html.

Applicable contractors are required to submit their Total Case Incident Rate (TCIR) and Days Away Restricted or Transferred (DART) rates and OSHA Form 300A annually to the contracting officer for consolidation and submission as part of the installation's annual VPP Safety and Health Management report.

An applicable contractor's VPP must identify the processes and procedures the contractor will use to track compliance with the Safety and Health Plan, and the process and procedures that will be used to correct violations.

It is the applicable contractor's sole responsibility for compliance with the OSHA (Public Law 91-596). The contractor must submit a Safety and Health Plan and corresponding site safety checklist to the Government Program Manager 10 days after contract award. The contractor's plan shall include appropriate measures to ensure the contractor reacts promptly to investigate, correct and track alleged safety and health violations and/or uncontrolled hazards in contractor work areas. Additional, installation specific references and policies may be included/attached to the delivery order. The plan shall:

- Demonstrate a management commitment to employee safety and health;
- Identify the application of the safety and health plan to subcontractors;
- Identify the roles and responsibilities of the following individuals:
  - Management;
  - Supervisors;
  - Employees
  - Safety Coordinator;
- Identify applicable safety rules and regulations;
- Include a worksite hazard analysis to include base-line hazard identification and required control measures;
- Include a job site analysis to include hazards to tasks required to control measures;
- Identify employee safety and health training requirements and the documentation process;

- Include a workplace inspection frequency, to include identifying the individual conducting the inspections;
- Include employee hazard reporting procedures;
- Identifies individual(s) responsible for corrective action hazards;
- Identifies first aid/injury procedures;
- Identifies procedures for accident investigation and report;
- Identifies emergency response procedures; and
- Identifies the process for tracking controlled hazards in contractor work areas

An applicable contractor is responsible for establishing these requirements for all sub-contractor who qualify as applicable contractors under the resulting contract.

The Contractor shall ensure its employees and subcontractors promptly report pertinent facts regarding mishaps involving reportable damage or injury to the AFRL Safety Office and the COR, and cooperate (IAW AFI 91-204) in any Air Force safety investigation and shall comply with the Contractor's safety and health plan.

7.0 Government Furnished Resources

The government will furnish the following "as is" at no cost to the contractor for their use in direct support of tasks outlined in this PWS:

- Adequate facilities that include office space and furnishings shall be provided for on-site members of the staff assigned to the program. The government shall decide the internal facility location for the contractor operations. Government personnel, such as the COR, can decide to reside in the same general office area as the contractor to facilitate a cooperative relationship between the contractor and the government. The contractor shall keep all office, work space and communications rooms free from clutter and adhering to Air Force standards for safety and security.
- Custodial services for any identified facilities.
- Local and long-distance phone service, fax machine, and reproduction machine in or near occupied facilities.
- Miscellaneous office supplies.
- Government forms, publications, and documents, if required.

- Computers, common use software, communication networks, and other resources owned or leased by the government for use by on-site contractor personnel as approved by the COR.
- The government shall furnish utilities at no cost to the contractor for performance of this order if performed in a government-owned or leased facility.

The contractor shall conform to the provisions of Air Force Instructions for safeguarding the government-furnished facilities and material contained herein.

Desk Telephones

Government telephones are provided for use in conducting official business. Contractor personnel are permitted to make calls that are considered necessary and in the interest of the Government. The contractor shall follow the same policies as Government personnel for telephone usage.

Mobile/Wireless Telephones and Smart Devices

Government issued mobile/wireless telephone and smart devices may be assigned to contractor personnel when the Government determines it is in the Government's best interest. Contractor personnel are prohibited from using any Government issued device for personal use.

Electronic Mail (E-mail)

All Government e-mail access and use by contractor personnel shall be in support of the individual's official duties and contract/order responsibilities. All information that is created, transmitted, received, obtained, or accessed in any way or captured electronically using Government e-mail systems is the property of the Government. Contractor personnel are prohibited from forwarding e-mail generated from a Government provided e-mail account to personal devices.

Copiers and Fax Machines

Copiers are to be used to copy material for official Government business only in the performance of the contract/order. Contractor personnel shall not use fax machines for other than official Government business in the performance of the tasks in the contract/order.

Computer and Internet

All Internet and electronic media access accomplished by contractor personnel (utilizing Government furnished equipment) shall be for official Government business in the performance of the tasks in the contract/order.

Canvassing, Soliciting, or Selling

Contractor personnel shall not engage in private activities for personal gain or any other unauthorized purpose while on Government-owned or leased property, nor may Government time or equipment be utilized for these purposes.

Security Violations Using Government Equipment

Any contractor violating Government security policies, guidelines, procedures, or requirements while using Government equipment or while accessing the Government network may, without notice, have their computer and network access terminated, be escorted from their work location, and have their physical access to their work location removed at the discretion of the CO/COR. The CO/COR will notify the contractor of the security violation and request immediate removal of the contractor employee.

Validation of Government Furnished Items (GFI) and Equipment Inventory

The contractor shall develop and maintain a complete GFI inventory that shall be made available to the Government upon request. Within three (3) business days of receipt of any GFI, the contractor shall validate the accuracy of the materials and notify the COR and/or other

identified Government representatives, in writing, of any discrepancies, and update the GFI inventory list.

NOTE: Validation shall consist of the contractor checking for physical and logical completeness and accuracy. Physical completeness and accuracy shall be determined when all materials defined as Government furnished are provided. Logical completeness and accuracy shall be determined when all materials defined and associated with a program, system, or work package are provided.

8.0 Contractor Furnished Resources

Not applicable.

9.0 General Information

The following establishes the general requirements and guidelines governing the performance of the tasks outlined in this PWS.

9.1 Place of Performance

The primary work location under this PWS is WP AFB, Dayton, Ohio, Area B, Building 676 with occasional meetings in buildings 15 and 16 or other AFRL WPAFB facilities. Any deviation requires prior approval from the Contracting Officer.

In the event an emergency is declared for Dayton, Ohio necessitating the implementation of an alternate work location, services provided under the contract may require implementation of an alternate work location. The Contracting Officer will make notification to the Contractor's business Point of Contact (see section 12.0). A modified work location will be adopted for the duration of the declared emergency, and the contractor shall comply with the provisions of that alternate work location.

The CO/COR may require the contractor to periodically use an alternate work location for testing and reporting on AFRL Continuity of Operations (COOP) or enterprise telework procedures and capabilities (shall not exceed 2 days per month per person unless directed by the Contracting Officer).

The contractors shall be responsible for assisting with or accomplishing end-of-day security checks for their room in bldg 676 if no government person is present at the end of the day.

For the classified processing facilities located in Bldg 676, services include, but are not limited to, escorting customers performing work, opening and closing room on as-needed basis, arming and disarming Intrusion Detection Systems (IDSs) and alarms, retrieving and storing classified data files.

9.2 Government Management

The AFRL Information Technology Strategy and Policy Division (AFRL/RCC), within the AFRL Research Computing and Collaboration Directorate (RC), will serve as the lead for the management of this contract.

9.3 Non-Disclosure Agreements (NDAs)

All contractor personnel that have potential access to government-only restricted information and files because of their system administrative or application administrative privileges shall sign a Non-Disclosure Agreement (NDA) with AFRL. The NDA shall state that government-only information shall not be shared with the employee's employer. NDAs must be signed before system administrative or privileged access for contractor personnel may be granted. These NDAs will be kept on file with the official contract folder and records or in the electronic records for the contract.

9.4 Normal Duty Hours

The contractor personnel are expected to perform their work within AFRL’s normal operating hours of 0700 to 1800, Monday through Friday, excluding government observed holidays. WP AFB and the AFRL support a flexible work schedule. Full time contractors working the normal shift are expected to arrive no later than 0900hrs and leave no earlier than 1500hrs (AFRL's core hours) unless approved by the COR on a case by case basis. If variances are required from the core operating hours, the contractor shall obtain permission from the COR prior to working those hours.

9.5 Extended Hours and Surge Support

Extended hours are rare; however, if additional extended hours support is needed beyond the normal performance within the order, such support will be identified in advance to the contractor and shall be funded by a separate time and materials Contract Line Item (CLIN). This effort may also include additional temporary support to accomplish special studies on topics of interest to the AFRL enterprise. For example, this could be to bring in a subject matter expert for 3 to 6 months to assist in the production of a report on some topic.

It is anticipated that the workload will increase above the Core Support provided via CLIN 0001 and 0002 and surge support may be required based on fluid schedule requirements. In anticipation of this increase, additional support required will be obtained via the utilization of CLIN 0003 – T&M Surge. Such support may encompass the entire scope of work identified as CLIN 0001 or CLIN 0002 - Core Labor. The Surge ceiling as identified in the FON will become the ceiling basis for any and all future tasks exercised. No surge requirements will extend beyond the period of performance of the CORE (CLIN 0001) effort. To ensure maximum flexibility, the contractor shall include a complete price list identifying the proposed Firm Fixed Price hourly labor rates for all labor categories to support CLIN 0001 - Core Labor, for the life of the task order. Prior to exercising this CLIN, the Government will identify a need that cannot satisfactorily be met with the staffing baseline as provided in staffing quote, or otherwise amended. The primary basis for the determination that the "additional workload" associated with such need falls into the optional surge labor CLIN vs. the core labor CLIN would largely be due to the determination that the labor mix and level of effort (i.e. accepted staffing plan that formed the staffing baseline) for the core labor incorporated into the original task order award isn't sufficient to perform the additional workload (e.g. potential new large-scale security constructs, subject matter expertise related to specialized short-term initiatives, mandated project schedule compression, etc.). A bilateral agreement will be reached between the parties to Firm Fix Price the effort requested using the labor categories and labor rates previously negotiated at award. This process may continue in any increment until the entire ceiling has been expended. The lifecycle ceiling for this CLIN will not increase without applying additional requirements found in the FAR.

9.6 Materials Purchasing – CLIN 0004

The contractor may require various minor materials and small equipment to complete their tasks in a timely manner. An Other Direct Costs (ODC) CLIN will be established for this purpose. The COR must approve all purchases before being made. The contractor shall not purchase items in excess of $3500 for a single purchase without the prior approval of the Contracting Officer (CO). Larger components and systems will be purchased under a separate contract and provided by the government. This CLIN will be focused on the purchase of small items, components, or software (for example: KVM switches, computer memory (RAM), hard drives, etc.) to support capability integration efforts, system upgrade efforts, or to rapidly replace failed components in the ELSZ to return the system to operational status.

9.7 Travel – CLIN 0005

Travel must be coordinated and authorized by the CO, the COR, and/or other identified Government representatives prior to incurring costs. Contractor costs for travel will be reimbursed in accordance with FAR 31.205-46, in arrears. The travel costs shall be reasonable

and allowable as defined in FAR 31.201 and in accordance with the limitations of the Joint Travel Regulation (JTR).

The contractor shall invoice monthly on the basis of cost incurred. The contractor must provide documentation in support of all travel expenses. The contactor will not be reimbursed for local travel (within a 50-mile radius of the Government/contractor's facility) or commuter travel (commute from home to work site).

Invoice submissions including travel costs shall include completed travel expense sheets (i.e., travel voucher) for each trip and each employee who traveled. The travel expense report, receipts of $75 or more (with exceptions being lodging and transportation), and supporting documentation (e.g., approval email for exceeding per diem rates, cost comparisons, etc.) shall be submitted with the invoice. Expense report(s) must include the traveler's name, dates of travel, destination, purpose of travel, Approval Authority documentation (e.g., copy of the e-mail authorizing travel by Government official), and cost for each trip. All travel costs shall be compiled into the Government provided travel expense sheet (**PWS Attachment D**) or similar document that has been determined to be acceptable by the Government. The entire submission shall be complete and organized to enable the Government to complete an efficient review. Submissions that are not complete and organized are subject to rejection.

Projected Travel. The following trip schedule is representative of the annual trips expected per year. It should be noted that this is a projection and the overall travel could be more or less than what is outlined in the below chart.

Number of People	Number of Trips per Year Expected	Reason	Typical Location
2	20	Site visit to support isolated interconnects	Various locations

Number of People	Number of Trips per Year Expected	Reason	Typical Location
		and classified interconnects setup	

9.9. Initial Business/Kickoff Meeting

Within 15 business days following the contract/order award (or other time mutually agreed between the parties), the contractor shall meet with the GSA CO, GSA COR, and other identified Government representatives to ensure a common understanding of the requirements, goals, expectations, end products, and objectives of the contract/order. The contractor shall discuss the overall understanding of the project and review the background information and materials provided by the Government. Discussions will also include the scope of work, deliverables to be produced, how the efforts will be organized and project conducted; assumptions made/expected end results. A concerted effort shall be made to gain a thorough understanding of the Government expectations. However, nothing discussed in this or in any subsequent meetings or discussions between the Government and the contractor shall be construed as adding, deleting, or modifying any contract/order requirements, including deliverable specifications and due dates. The contractor shall also address the status of any issues that will affect contractor start-up/ramp-up toward achieving full service/support capability. The contractor will be responsible for taking minutes of this meeting.

10.0 Contractor Employee and Training Requirements

The contractor shall provide necessary personnel to accomplish all work identified in the PWS.

The contractor shall provide personnel with the necessary licenses, certifications, training, experience levels, and security clearances that are required, including Federal, State, and local laws and regulations including the requirements to satisfy DOD Directive 8140.01 (or future policies that may supersede DoDD 8140.01). Fulfilling CyberSecurity (IA) certification program continuing education requirements is the responsibility of the contractor. Contractor positions under this effort, as identified in DoDD 8140.01 shall all be at Information Assurance Technical (IAT) level II.

The government may consider funding of contractor training only for government unique or specialized needs. All requests for training at government's expense shall be submitted to the COR for approval or disapproval prior to training.

The contractor shall be responsible for all cost including labor hours associated with the equivalent training of replacement personnel when contractor personnel who have received government-funded training leave and are replaced. The contractor shall train replacement personnel for seamless support of IT services under this order. The training shall be provided within one month of employee's arrival at AFRL. The contractor shall provide training documentation/certification in the monthly status report.

Each person shall be required to identify themselves as contractor employees in all written correspondence, telephone conversations, and when attending government meetings.

Contractor employees shall follow direction of emergency personnel or AFRL management in the event of actual or simulated fires, weather advisories, natural disasters, bomb threats, terrorist activities, enemy attack, and other similar emergency type conditions posing a real or potential danger to people or property. Contractor shall provide in-house security and disaster training to their employees at contractor's expense.

11.0 Contractor Point of Contact (POC)

The contractor shall identify one employee as the Contractor POC and one employee as an alternate. This will be the individual that will coordinate with the government in matters of contract performance. Written notification of the name, address, home telephone and mobile telephone of the Contractor POC and an alternate shall be provided to the AFRL Contracting Officer and COR the first day of order performance and thereafter as changes occurs. This individual or in his or her absence, the designated alternate, shall have full authority to act for the contractor on all matters relating to the day to day operations of the contract.

12.0 Security and Identification Procedures

Contractor personnel working on classified material or having access to classified materials or facilities shall have a security clearance at the required level. Secret clearance is required for access to Secret materials. Top Secret clearance is required for access to Top Secret materials as well as a "need to know". Clearance levels are identified in the estimated manning levels. The contractor shall coordinate with the AFRL headquarters security manager prior to accessing any classified material or accessing any classified facilities.

DoD military, civilian, consultants, and contractor personnel using unclassified automated information systems, including e-mail, must have, at a minimum, a current DoD Secret security clearance in accordance with DoD 5200.2-R Personnel Security Program, January 1987. Copies of the completed application documents and forms shall be furnished to the AFRL Security Manager and the COR at least two days prior to the start of work.

The Contractor POC or Alternate shall provide to the AFRL headquarters Security Manager, a completed DD Form 1172-2, Application for Department of Defense Common Access Card-DEERS and DD Form 2842, DoD Public Key Infrastructure (PKI) Subscriber Certificate Acceptance and Acknowledgement of Responsibilities for each contractor employee requiring access to AFRL or any other Government installation. The government shall provide a completed Identification Credential, AFMC Form 387, which shall be issued, displayed and surrendered as directed in AFI 31-101, Integrated Defense (FOUO). When contractor employees no longer support this order, the contractor shall immediately surrender all subject employee government issued identification badges to the AFRL Security Manager.

The contractor shall ensure all employees properly display and wear locally authorized Identification (ID) Badges at all times during duty performance of this order. Contractor employees shall be easily recognized as contractor employees with a local ID Badge that includes, as a minimum, a person's name, the name of the contractor, and the word "Contractor." Each employee shall wear the local Badge on the outer clothing on the front of the body between the neck and the waist so that the ID Badge is visible at all times. (Note: If wearing an ID Badge jeopardizes safety of contractor personnel in performance of their duties, the Badge will be removed until the job is completed and the hazard is no longer present.) When contractor employees no longer support this order, the contractor shall immediately surrender all subject employee government issued identification badges to the AFRL headquarters Security Manager.

Each person will identify themselves as a contractor employee in all written correspondence and telephone conversations.

The contractor shall observe and comply with all DoD, USAF, AFMC, and AFRL security provisions in effect during the order period of performance.

Due to the sensitive nature of work to be performed on this effort, the contractor shall employ U.S. citizens only.

DoD Cybersecurity training, as required by the AFRL or USAF Cybersecurity offices, shall be taken and must be passed by all on-site contractor personnel.

The Contractor shall ensure that personnel accessing information systems have the proper and current cybersecurity certification to perform cybersecurity functions in accordance with DOD Directive 8140.01 or future policies that may supersede DoDD 8140.01. The Contractor shall meet the applicable cybersecurity certification requirements, including—

(1) DoD-approved cybersecurity workforce certifications appropriate for each category and level as listed in the current version of DOD Directive 8140.01 or future policies that may supersede DoDD 8140.01; and

(2) Appropriate operating system certification for cybersecurity technical positions as required by DOD Directive 8140.01 or future policies that may supersede DoDD 8140.01.

The Contractor shall provide documentation supporting the cybersecurity certification status of personnel performing cybersecurity functions in the staffing plan.

Contractor personnel who do not have proper and current certifications shall be denied access to DoD information systems for the purpose of performing cybersecurity functions.

Contractor shall participate in the organization's OPSEC Program. OPSEC requirements are required in an effort to reduce program vulnerability from successful adversary collection and exploitation of critical information. The contractor shall apply OPSEC in their management of this program IAW AFI 10-701 Operations Security and the AFRL/RC OPSEC Plan.

Privacy Act: Work on this project may require that contractor personnel have access to information which is subject to the Privacy Act of 1974. Personnel shall adhere to the Privacy act, Title 5 of the U.S. Code, Section 552a and applicable agency rules and regulations when handling this information. Privacy Act information is considered sensitive and appropriate safeguards shall be implemented by the contractor. The contractor is responsible for ensuring all contractor personnel are briefed on privacy Act requirements.

14.0 Quality Control

Contractor shall develop and maintain a quality program to ensure services are performed in accordance with commonly accepted commercial practices. Contractor shall develop and implement procedures to identify, prevent, and ensure non-recurrence of defective services. As a minimum, the contractor shall develop quality control procedures that address the areas identified in Section 6.0, Service Delivery Summary.

15.0 Quality Assurance

The government will evaluate the contractor performance IAW the PWS and the Quality Assurance Surveillance Plan (QASP).

16.0 Performance of Services During Emergency Conditions

In the event an emergency is declared for Dayton, Ohio necessitating the implementation of an alternate work schedule (other than a standard 8 hour day, Monday through Friday workweek), services provided under the order may require implementation of an alternate work schedule, not to exceed a 40-hour workweek. The Contracting Officer will make notification to the Contractor's business point of contact. A modified work schedule will be adopted for the duration of the declared emergency, and the contractor shall comply with the provisions of that alternate work schedule.

In the event that the base is closed by the base Commander due to weather conditions and travel on roadways is deemed dangerous, the contractors are excused from duty while the base is closed. In the event of a Government Shutdown the Contractor shall receive notice from the COR on how to proceed.

17.0 Contractor Manpower Reporting Using eCMRA

Section 2330a of title 10, United States Code (10 USC 2330a), requires the Secretary of Defense to submit to Congress an annual inventory of contracts for services performed during the prior fiscal year for or on behalf of the Department of Defense (DoD). The inventory must include the number of contractor employees using direct labor hours and associated cost data collected from contractors. The contractor shall use the Air Force portion of the Contractor Manpower Reporting Application (eCMRA) to report ALL contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract for the Air Force via a secure data collection site. This statutory reporting also requires the contractor's compliance with the following subparagraphs.

The contractor shall completely fill in all required data fields at http://www.ecmra.mil/

The contractor's reporting inputs shall be for the labor executed during the period of performance for each government fiscal year (FY), which runs 1 October through 30 September.

While inputs may be reported any time during the FY, all data shall be reported no later than 31 October of each calendar year.

The contractor is advised information from the secure eCMRA web site is considered to be proprietary in nature when the contract number and contractor identity are associated with the direct labor hours and direct labor dollars. At no time will any data be released to the public with the contractor name and contract number associated with the data. Data for Air Force service requirements must be input at the Air Force CMRA link which is accessible from the main eCMRA web site. User manuals for government personnel and contractors are available at the Army CMRA link. The contractor shall direct any eCMRA questions to the CMRA help desk at http://www.ecmra.mil.

The contractor shall notify the COR each calendar year that the eCMRA data for the previous fiscal year was submitted on time. This notification shall be submitted as part of the Oct monthly report for that year.

18.0 System Transition

In the event of a transition between support contractors at the end of this contract – the contractor shall ensure a smooth system transition is accomplished to the receiving contractor. If there is no transition to a new support contractor at the end of this contract – then this section (19.0) is not applicable.

Phase-In Plan

The contractor may or may not propose a separately priced transition period, for a duration to be determined and proposed by the contractor, but shall not exceed a period of 2 calendar days. The transition period is defined as the period of time (during the phase-in) when the new contractor and the incumbent contractor will both be providing support to the client as required to support the transition to the newly awarded contract/order. If the contractor chooses to propose a transition period, such period shall be included and addressed within the below identified phase-in plan.

The contractor shall develop a phase-in plan. Such phase-in plan shall present a clear understanding of the phase-in tasks required, the issues likely to result from non-incumbent contractor performance, and the contractor's proposal to resolve such issues. The phase-in plan shall include a clear and feasible strategy for delivering services required within the periods

specified by the plan and shall include a detailed plan-of-action and milestones to transition the functions identified in this PWS in a well-planned, orderly, and efficient manner. The phase-in plan shall include, at a minimum:

- Staffing plan.
- Development and submission of required deliverables.
- Interface with the Government and incumbent contractor (if applicable) during phase-in, to include meetings or status reports, as required.
- Approach to maintaining quality and minimizing disruption during phase-in.
- Development and dissemination of operating instructions, procedures, and control directives.

In the event of a transition between support contractors at the end of this contract – the Contractor shall prepare and deliver a non-proprietary Contract Transition Plan (CTP) no later than 60 calendar days prior to the end of the Period of Performance (PoP) of the contract for the orderly transfer of all items related to the continued sustainment and maintenance of the ELSZ system. The CTP shall include a description of the activities and schedule required to transition the maintenance, sustainment, and technical support functions from the current Contractor(s) to the follow-on Contractor or Government agency. The CTP shall cover no less than a one-month period, to include assisting a follow-on Contractor through the transition process (CDRL A003). This plan should detail the activities needed to support the following phase-out requirements:

- Apply all current OS upgrades, patches and TCNOs
- Apply all current application patches and TCNOs
- Back-up all Virtual Servers, applications, databases, and user data and provide this backup on tape and or USB hard drive
- Provide detailed inventory list of operating systems, software, versions, and TCNO’s on servers
- Provide detailed inventory list of all Government software, licenses, hardware, and equipment
- Provide copies of all documentation; operating and maintenance instructions; and operating and maintenance checklists

During the inventory, the Contractor and Government representative shall jointly determine and document the working order and condition of all property and notify the CO in writing within five (5) days of completion of the inventory. The Contractor has the responsibility to resolve any discrepancies between the joint inventory and official Government records.

The Contractor agrees to preserve and make available to the Contracting Officer, as requested, copies of all records and other documentation (electronic or as designated by the Contracting Officer), developed or acquired under this contract for this effort, regarding performance of the work required by this contract and support the transition activities associated with systems sustainment to the next Contractor.

19.0 Anticipated period of performance

REQUIREMENTS/PERFORMANCE STANDARDS

The anticipated period of performance is as follows:

Base Period: 1 Dec 2019 – 31 May 2020 (six months)

Option 1: 1 Jun 2020 – 31 May 2021 (one year)

Option 2: 1 Jun 2021 – 31 May 2022 (one year)

Option 3: 1 Jun 2022 – 31 May 2023 (one year)

Option 4: 1 Jun 2023 – 31 May 2024 (one year)

20.0 Critical skills for this effort

- The ability to manage an enterprise IT environment comprised of mostly Linux and Open Source Software with some Microsoft Windows servers and other commercial software.
- The ability to manage a virtualized data center across multiple security classification levels up to and eventually including Top Secret.
- Experience with operating and maintaining IT systems in a DoD environment.
- Experience with operating and maintaining IT systems in a research or academic environment.
- Experience with DoD or AFRL Risk Management Framework (RMF) and hardening and operating IT systems accordingly. Experience with the application of the DISA Security Technical Implementation Guides (STIGs).
- Experience with data center level hardware including blade servers, high speed fiber optic based networking, and Storage Area Networks (SANs).
- Experience with DevOps paradigm for data center operations and automated system provisioning and configuration management using Puppet/Foreman.
- Experience with helpdesk support of a highly technical, geographically distributed user-base (DoD scientists, engineers, and developers).

21.0 Anticipated Hardware and Software to be Supported

21.1 Representative Hardware

The following is representative of the hardware that the contractor shall be responsible for operating and maintaining – but may not be all inclusive.

- Blade server chassis with embedded network switches (currently the HP C7000 chassis with HP blade servers)

- Network Attached Storage heads and Storage Area Network expansion blocks (currently the Dell FS7610 NAS heads, Equallogic SAN blocks, and Dell 10Gbps network switches)
- Tape libraries (currently the HP tape libraries with multiple drives and robotic tape changers)
- TACLANE encryption devices
- Firewall/VPN appliances for wide area isolated network interconnects and network and traffic segregation behind the TACLANE encryptors (currently Fortinet FortiGate 200G and 100EF appliances)
- Top of rack network switches (currently Cisco Nexus switches)
- Enterprise RDT&E Firewall (currently a Cisco ASA)

21.2 Representative Software

The following is representative of the software that the contractor shall be responsible for operating and maintaining – but may not be all inclusive.

- XenServer and/or VMWare as the type 1 hypervisor
- Kubernetes
- OpenStack
- CentOS Linux 7.x for workstations, servers, and virtual servers
- Puppet/Foreman for system provisioning and configuration management and DISA STIG application
- Apache and NGINX for web servers
- MySQL, MariaDB, and PostgreSQL for database servers
- Tiki, MediaWik, NextCloud, osTicket, GitLab Enterprise, and Moodle for web applications
- PHP, Python, Ruby, Java, and Javascript for application development languages
- Microsoft Windows Server 2016 with Active Directory for authentication services
- Nagios or similar applications for system and service monitoring and dashboarding
- ACAS, Nessus or OpenVAS or similar applications for vulnerability scanning
- GEM for TACLANE remote management

- AlienVault Security Information and Event Management (SIEM) system
- OSSEC, OCS Inventory NG, Nagios, and Puppet client software installation, configuration, and management

PERSONNEL

General Requirements

All contractor personnel shall meet the minimum general requirements listed below.

- All personnel shall be capable of working independently.
- All personnel shall have training and experience that is appropriate for the tasks to which they will be assigned.
- The contractor shall provide personnel that are capable of conducting themselves in a professional manner and have proper telephone and e-mail etiquette, customer service techniques, and organizational skills
- Strong written and oral communication skills in the English language. All contractor personnel must be able to read, write, speak and understand English.
- Contractor personnel performing in a leadership capacity shall be capable of directing contractor personnel and interfacing with the Government and customers.
- Exceptional customer service skills.
- Strong time-management and prioritization skills.
- Ability to communicate applicable technical subject matter expertise to management and others.

1.1 Specific Expertise and Experience

The contractor shall provide personnel with the appropriate skill levels. While each individual contractor employee may not possess expertise and experience in each area below, the Government requires that the overall contractor staff possess the aggregate skills, expertise, and experience in each of the areas identified to successfully complete all requirements. **All personnel must meet DoD 8570 (or DoD 8140 when superseded) requirements PRIOR to being granted elevated privileges.** All DoD 8570/8140 positions covered by this contract will be at IAT level II.

- Linux Systems Administrators (DOD 8570/8410 IAT Level II requirements)

- Minimum of CompTIA Linux+ or equivalent certification
- Minimum of CompTIA Security+ certification

- Microsoft Systems Administrators (DOD 8570/8410 IAT Level II requirements)
  - Minimum of Microsoft Windows Server certification
  - Minimum of CompTIA Security+ certification
- Network Engineer
  - Minimum of a Cisco Certified Network Engineer (CCNE) certifications (all ELSZ and NOC network infrastructure is based on Cisco brand network equipment)
  - Minimum of CompTIA Security+ certification
- Cyber Security Specialist (DOD 8570/8410 IAT Level II requirements)
  - Minimum of Certified Information System Security Professional (CISSP)

1.2 Training

1.2.1 Contractor Staff Training

The contractor shall provide fully trained and experienced support staff. Contractor personnel are required to possess the skills necessary to support the minimum requirements of the labor category under which they are performing. Training of contractor personnel shall be performed at the contractor's expense, except when the Government changes the requirements during performance of an on-going task and it is determined to be in the best interest of the Government. This will be negotiated on a case-by-case basis. Training at Government expense will not be authorized for replacement personnel nor for the purpose of keeping contractor personnel abreast of advances in the state-of-the-art, or for training contractor personnel on equipment, computer languages, and computer operating systems that are available in the commercial market.

1.2.2 Mandatory Government Training

Mandatory Government training shall be tracked and monitored by the contractor. All required courses must be completed by the required dates by all contractor personnel. Mandatory Government training classes may be completed during work hours. It is the intent of the Government to provide 30 calendar days written notice of annual training requirements to the designated contractor representative. The designated contractor representative will be responsible for notifying subordinate contractor personnel. In the event the contractor does not receive a 30 calendar day notice, the contractor is still required to complete the training by the specified required date(s).

1.3 Key Positions / Key Personnel

Key personnel are personnel proposed to perform in key positions. Key positions are those deemed essential for successful contractor accomplishment of the work to be performed. The contractor shall identify the key positions associated with this contract.

Furthermore, the contractor is responsible for identifying key positions beyond those identified above, as applicable; within the contractor's respective proposed staffing plan (i.e. contractor identified key positions above and beyond the Government's identified requirements).

1.4 Personnel Retention and Recruitment

Government review and acceptance is required for all resumes of personnel proposed to support labor hour requirements and key personnel proposed to support all firm fixed priced requirements. The contractor shall make every effort to retain personnel in order to ensure continuity until contract/order completion. If it should become necessary to substitute or replace personnel, the contractor shall immediately notify the COR and/or other identified Government representatives in writing of any potential vacancies and shall submit the resume(s) of replacement personnel within 14 calendar days of the notification. Additionally, for all new positions identified by the Government, the contractor shall submit the resume(s) of proposed personnel within 14 business days of the Government's initial request. The contractor shall submit the resume(s) of all potential personnel selected to perform under the contract/order to the COR and/or other identified Government representatives through GSA's web-based procurement system, or any other process means identified/required, for Government review

and acceptance/rejection. Upon Government acceptance of a personnel resume(s), the candidate shall be available to begin performance within 14 business days. The contractor shall ensure continuity of operations during periods of personnel turnover and long-term absences. Long-term absences are considered those longer than one week in duration.

Contractor Performance Assessment Reporting System (CPARS) Assessment

Upon request by the Government, the contractor shall submit a self-evaluation of their performance at least annually utilizing a Government provided template. From time of Government request, the contractor shall have 7 business days to provide input to the GSA COR. The contractor self-assessment will then be submitted to the Government client where they will utilize this information to formulate an independent performance evaluation that will be processed through the Contractor Performance Assessment Reporting System. The requirements of the FAR and its supplements as it pertains to CPARS reporting shall be adhered to.

Personal Service

This is not a “Personal Services” contract as defined by FAR 37.104. Although contractor personnel who furnish services under the contract/order are subject to Government technical oversight, neither the Government nor a Government authorized third party contractor or representative shall oversee or supervise contractor personnel but shall provide all direction through the contractor’s designated representative(s) who is/are solely responsible for supervising and managing contractor personnel.

Section 508

Unless otherwise exempt, all services and/or products provided in response to this requirement shall comply with Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794d), and the Architectural and Transportation Barriers Compliance Board Electronic and Information Technology (EIT) Accessibility Standards (36 CFR part 1194).

Close-Out Procedures

The contractor is required as a deliverable of the contract/order to provide a final invoice no later than 30 calendar days after the end of the period of performance. Additionally, the contractor shall provide a Release of Claims no later than 90 calendar days after the end of the period of performance. The contract/order will be modified for closeout.

APPENDIX A: Environment Breadth and Complexity

A.1 AFRL RDT&E ELSZ

AFRL has created a collaborative and information sharing system focused on the specific and unique needs of AFRL's S&Es. There are five zones currently approved by AFRL leadership, but additional zones may be created depending on requirements and availability of funding. Each of the ELSZ zones will share a common core architecture unless an alternative is pre-approved by the ELSZ Program Manager. Approved mature, secure, and well maintained Open Source Software (OSS) will be evaluated and used whenever feasible to meet capability or infrastructure requirements. The work on this contract will cover all of the current and under construction zones as well as any future zones that might be established.

A.1.1 Current Approved Zones

A.1.1.1 Unclassified Extranet

The ELSZ Unclassified Extranet is a DREN connected environment that is intended to be accessible from anywhere AFRL S&Es need to work from, as well as from sites where there are external partners and customers, such as contractor sites, universities, other DoD agencies, and other Federal organizations (NASA, Department of Energy, Department of Homeland Security, etc.).

A.1.1.2 Unclassified Isolated Intranet

The ELSZ Unclassified Isolated Intranet is designed to provide the same services as the Unclassified Extranet, but for those AFRL RDT&E isolated, stand-alone, or segregated networks that voluntarily choose to interconnect into an AFRL-wide segregated network. In addition to the core Extranet collaboration capabilities, the unclassified isolated intranet will also provide some communication capabilities, such as email, instant messaging, and virtual meetings, which are not otherwise accessible to the isolated environments. These communication capabilities will be limited to isolated-to-isolated.

A.1.1.3 Classified (Collateral Secret) Isolated Intranet

The ELSZ Classified (Collateral Secret) Isolated Intranet is designed to provide the same services as the unclassified isolated intranet, but for those AFRL RDT&E and external partner isolated classified network enclaves that will be interconnected into a wide-area classified isolated RDT&E environment.

A.1.1.4 Virtual Machine (VM) Hosting Sandbox (currently under construction)

The VM Hosting Sandbox is intended to provide a segregated network area to host AFRL S&E prototype or experimental virtual machines to support software development, concept exploration, software evaluations, continuous integration, and capability evaluation. The environment is not intended for production or permanent servers (except perhaps continuous integration support systems). Access to the environment, by either AFRL S&Es or by external partners or customers, requires a secure client VPN connection.

The environment will support a mix of traditional 'thick' virtual machines and containerized virtual machines (Docker or similar). AFRL S&Es must be allowed to have full control of, and access to, their virtual machines. The virtual machines connectivity must be configurable to allow: no external connections; connections to other virtual machines; or outbound-only connectivity to the Internet. Access to outside networks such as the Internet or DREN will be restricted or limited at the discretion of the ELSZ program manager and/or Information System Security Manager (ISSM).

A.1.1.5 Classified (Top Secret SCI) Isolated Intranet (construction to start in FY20)

The ELSZ Classified (Top Secret SCI) Isolated Intranet is designed to provide the same services as the unclassified isolated intranet, but for those AFRL RDT&E and external partner isolated classified network enclaves that will be interconnected into a wide-area classified isolated RDT&E environment at the Top Secret SCI level.

A.1.2 Current Core Capabilities

The contractor will be responsible for implementing, operating, maintaining, and securing all of the current, and future, ELSZ applications.

Users access the ELSZ services from a variety of RDT&E platforms, operating systems, and application software. Every ELSZ service will be open standards based and will be user platform/operating system/application agnostic. ELSZ services must not require or mandate a particular operating system, web browser, or other client software application in order to use the provided services.

A.1.2.1 Large File Transfer and Sharing

AFRL S&Es need a method of transferring and sharing very large data files and very large sets of files. The ELSZ Program has implemented two different methods of large file transfer:

Secure File Transfer Protocol (SFTP)

SFTP is very well suited to transferring very large individual files (up to 2 terabytes (TB) individual files tested) as well as very large sets of files (up to 10TB file batches tested). The disadvantage for users is that it requires an additional client application on the user end. Also, currently the ELSZ system administrators must manage the access groups and permission structure on shared files and folders. The ELSZ SFTP capabilities have been implemented using open standard protocols so that the service can be used with any open standards compliant user application. The ELSZ SFTP capability is implemented to support Common Access Card (CAC) based key authentication, self generated Secure Shell (SSH) based key authentication, and username-password authentication. Username-password authentication will be phased out at the earliest opportunity. Since very large file transfers can take more than 8 hours, the ELSZ SFTP system will always support SSH-key based authentication. The ELSZ SFTP capability will also support SSH File System (SSHFS) connectivity to support remote mounting of the file storage areas as client local directories. The ELSZ SFTP server has access to a Storage Area Network (SAN) based file system that currently has hundreds of TB of storage and can be expanded to petabytes of storage.

Web-based File Sharing (NextCloud)

The current ELSZ web based file sharing and transfer capability has been implemented with an Open Source Software application called NextCloud (https://nextcloud.com/). This capability has been tested with individual files up to 20 gigabytes (GB) in size and only requires an open standards compliant web browser to use. The ELSZ NextCloud web based file sharing capability has access to the same large file volume as the SFTP based capability. Users are able to share files and folders, create directory structures, and set or view permissions without intervention by the ELSZ systems administrators. Users may also share files or directories 'by link' to allow sharing with external users that do not have an ELSZ account but do have a DoD CAC or DoD Public Key Infrastructure (PKI) certificate.

A.1.2.2 Distributed Software Development

AFRL S&Es need tools to support software development with teams distributed within their TDs, between sites, and even with external partners.

GitLab Enterprise

The commercial, but partly open source software, GitLab Enterprise application (https://about.gitlab.com/features/) was chosen for implementation to support the distributed software development requirement. GitLab has a similar web based user interface to GitHub

which many software developers are familiar with while using open standards based Git at its core.

A.1.2.3 Web-based collaboration

Current limitations in the mainstream AF and DoD web collaboration capabilities necessitate additional capabilities to meet AFRL S&E's specific needs for research collaboration. Specifically the current AF and DOD collaboration capabilities are limited in the individual file sizes they can support as well as the total volume of data that can be stored within any given site.

Tiki

The Open Source Software Tiki (formerly known as TikiWiki) web based groupware and collaboration application (https://doc.tiki.org/features) is similar in functionality to Microsoft Sharepoint – however Tiki, for example, can support sharing individual files up to 6GB in size and is not limited in the total amount of files that can be stored. Tiki offers a diverse set of tools to meet the AFRL S&Es collaboration requirements including a very feature rich Wiki capability supporting numerous plugins (https://doc.tiki.org/tiki-index.php?page=Wiki Plugins) and dynamic content. The Tiki application also allows very fine grain permission control (https://doc.tiki.org/Permissions) by users at the content and file level.

Media Wiki

The Open Source Software MediaWiki (https://www.mediawiki.org/wiki/MediaWiki) capability allows supported groups to develop and distribute information related to their group in a familiar format. The MediaWiki 'sites' will be accessible to anyone who can CAC or PKI authenticate to the ELSZ environment but authoring content will be restricted to those with ELSZ accounts.

A.1.2.4 Email List Serving (Mailman)

The current AF email system does not easily allow for the creation of email distribution lists with users not in the AF global address list, nor does it support lists with multiple owners, nor does it provide an archive of messages sent to the list. To meet the needs of AFRL S&Es to collaborate with external partners, the ELSZ program has implemented an email list server based on the Mailman Open Source Software application (http://list.org/). Mailman provides a web based interface for list owners to create and manage their project or working group lists.

A.1.3 Current Additional Isolated-Only Services

Since the unclassified and classified isolated network environments do not have access to the communication tools on the NIPRNET and DREN, but still have a requirement to communicate between them, a set of tools to provides these capabilities have been implemented in the

corresponding ELSZ zones. They are intended for isolated lab to isolated lab communication as well as process or experiment to S&E notifications. No traffic from outside networks, such as NIPRNET, DREN, or the Internet, can enter the isolated environment and no internal communications can leave the isolated environment.

A.1.3.1 Isolated-to-isolated Email

Since the AFRL RDT&E isolated or segregated network environments do not have access to the AF email system, ELSZ provides an isolated-to-isolated email capability. This email capability supports open standards based client connectivity as well as a web-mail capability.

A.1.3.2 Isolated-to-isolated Instant Messaging

Since the AFRL RDT&E isolated or segregated network environments do not have access to the AF or DoD instant messaging system, ELSZ provides an isolated-to-isolated instant messaging capability. This capability supports open standards based client connectivity. The current capability utilizes NextCloud (https://nextcloud.com/talk/), but the contractor will implement a full Extensible Messaging and Presence Protocol (XMPP) based instant messaging capability with full presence functionality.

A.1.3.3 Isolated-to-isolated Virtual Meetings

A key requirement of the interconnected isolated environments is to support desktop-based audio-video calling with shared screens – something similar to a web-based Skype or Google Hangouts type multiple participant virtual meeting capability. The capability needs to allow the researchers and developers to troubleshoot and assist each other with software installs and configurations. The current capability utilizes NextCloud (https://nextcloud.com/talk/).

A.1.4 Possible Future Expansion

A.1.4.1 Possible Future Zones

The ELSZ Program Manager may authorize the contractor to implement an additional Above Secret zone. This will require support personnel with at least Top Secret security clearances.

A.1.4.2 Possible Future Capabilities

A.1.4.2.1 Comprehensive Search

The ELSZ Program Manager may authorize the contractor to implement a comprehensive search capability to allow users to find information anywhere across the various ELSZ capabilities.

A.2 AFRL RDT&E NOC

The AFRL RDT&E IT environment has become complex enough to necessitate the construction and operation of a centralized, enterprise NOC to provide standardized services to all AFRL RDT&E sites and network layers. Construction of the NOC system and capabilities will begin in FY20.

There are four environments currently approved by AFRL leadership (Unclassified DREN, Unclassified Isolated, Collateral Secret Isolated and Top Secret SCI Isolated) with construction to begin in FY20, but additional environments may be created depending on requirements and availability of funding. The infrastructure for each of the supported environments will share common core architecture. AFRL Enterprise Cyber Security Office approved mature, secure, and well maintained OSS will be evaluated and used whenever feasible to meet capability or infrastructure requirements. The work on this contract will cover all of the current environments as well as any future environments that might be established.

Some initial NOC-type capabilities have been developed under the ELSZ effort. These capabilities will be logically regrouped under the NOC and expanded.

A.2.1 Current Approved Environments

A.2.1.1 Unclassified DREN

Much of AFRL's RDT&E IT environment is connected to the DREN. Currently each site provides most or all of their required infrastructure capabilities individually and with little standardization. The enterprise RDT&E NOC will provide centralized enterprise services to AFRL's DREN connected enclaves.

The contractor will be responsible for implementing, operating, maintaining, and securing the core infrastructure services provided to these DREN connected enclaves.

A.2.1.2 Unclassified Isolated

In order to achieve maximum flexibility and the ability to run older and perhaps vulnerable operating systems and applications to support specific research functions, some of AFRL's research IT environment has moved to isolated/segregated or stand-alone enclaves. These enclaves provide segregation and reduced risk in some dimensions, however their isolation cuts them off from communications, collaboration, and infrastructure services such as updates to servers potentially increasing risk in other dimensions. (For example, AFRL's primary injection point for malware is the isolated and stand-alone networks.)

There is an ongoing effort to interconnect as many of these unclassified, isolated environments together, as possible, into a wide area isolated environment. This overall environment will still be isolated/segregated and systems on it will still not have access to outside networks such as NIPRNET, DREN, and the Internet. These interconnections are created using commercial VPN appliances which create exclusive encrypted tunnels between the networks while maintaining their external isolation. A firewall capability on the appliances can be used to control what traffic is allowed to and from connected systems.

The contractor will be responsible for implementing the wide-area unclassified isolated/segregated network, managing the remote VPN appliances, and implementing, operating, maintaining, and securing the core infrastructure services provided to these interconnected enclaves.

A.2.1.3 Classified (Collateral Secret) Isolated

Similar to the unclassified isolated environments, the classified isolated environments offer the same advantages and disadvantages, just at a higher security classification level.

Also similar is the ongoing effort to interconnect many of these remote classified isolated environments into a wide-area secure environment to support distributed development, collaboration, cooperative virtual simulations, etc. These interconnections are created using NSA approved TACLANE encryptors.

The contractor will be responsible for implementing the wide-area classified isolated/segregated network, managing the remote TACLANEs, and implementing, operating, maintaining, and securing the core infrastructure services provided to these interconnected enclaves.

A.2.2 Current Services

The contractor will implement and or maintain the following current services as well as any future services as yet to be determined.

A.2.2.1 Infrastructure Services

Authentication

The NOC will provide authentication services supporting username-password authentication as well as PKI certificate authentication across all of the supported environments. This authentication capability will support enterprise RDT&E capabilities such as the ELSZ services, but must also be usable by the AFRL Technology Directorates for their RDT&E enclaves local system authentication.

Domain Name Service (DNS)

The NOC will provide Domain Name Services (DNS) within each of the supported environments. A change management process will be developed to allow requests from the AFRL sites for new or updated entries.

Network Time Protocol Service (NTP)

The NOC will provide Network Time Protocol (NTP) service across all of the supported network environments. The NTP service will be provided with less than 10 seconds of drift per year to real time.

Encryptor/VPN management

The NOC will provide centralized configuration management of TACLANE encryptors and other commercial VPN appliances used to interconnect isolated RDT&E networks at either the classified or unclassified level. The contractor will review and update as necessary the firmware of all managed devices a minimum of once a quarter.

Automated IT Systems Lifecycle Management

The NOC will provide automated IT systems life-cycle and configuration management capabilities to support rapid RDT&E physical and virtual server and workstation provisioning, configuration, software installation, STIG application, and ongoing configuration management. (currently Puppet/Foreman – https://puppet.com/solutions/configuration-management - https://www.theforeman.org/). This capability will be usable within the Enterprise RDT&E IT environment for systems deployment and management, but must also be usable by remote AFRL Technology Directorates for local server and workstation deployment and management. The capability must allow for enterprise level configurations as well as local or lab or group specific configurations.

All ELSZ and NOC physical and virtual servers will utilize this capability to implement the greater majority of system configuration changes throughout their life-cycle. This capability will be used to spawn new virtual servers in both sides of the environment as necessary. This capability will be used to apply the DISA STIGs, as appropriate, to all physical and virtual servers in both sides of the environment.

A.2.2.2 Cyber Security Services

Update Services

The NOC will provide software, operating system, and anti-malware update services to all of the supported environments. This capability is particularly critical in the unclassified and

classified isolated environments where patching and updating systems is much more difficult since they cannot access outside update resources.

Linux Update Service

The NOC will provide Linux operating system and application software repository mirrors across all of its supported environments for a minimum of the following Linux distributions:

- CentOS Linux (including EPEL repository)
- Scientific Linux (including EPEL repository)
- Fedora
- OpenSUSE
- Ubuntu
- Debian

Updates to the repositories across all supported isolated environments will be accomplished a minimum of monthly. Additional repositories for other Linux distribution and or other versions of current Linux distributions will be created based on user request. The Linux repository mirrors will be usable for automated operating system and application updates by just changing the repository host name in the individual system updates (yum, apt, etc.) configuration.

Software Library Update Service

The NOC will provide software development library repository mirrors across all of its supported environments. The specific library repositories will be determined based on user needs, but some examples include but are not limited to: PERL (CPAN), Python (PyPI, SciPy, NumPy, and PIP), Ruby (RubyGems), and PHP repositories.

Updates to the repositories across all supported isolated environments will be accomplished a minimum of monthly. Additional repositories will be created based on user request.

Windows Update Service

The NOC will provide Windows Update Service (WUS) across all of its supported environments. Updates will be provided for a minimum of Windows 2000 version and forward – since many systems in the isolated environments can use very old operating systems.

Updates to the Windows Update Service will be accomplished a minimum of weekly on all supported isolated environments. Additional Windows or Microsoft software versions will be added based on user request.

Mac OS X Update Service

The NOC will investigate if a Mac OS X operating system update server can reasonably be created and maintained for the isolated environments, and if so, provide that service across all supported isolated environments.

If created, the Mac OS X update service will be updated a minimum of monthly on all supported isolated environments.

Anti Virus / Anti Malware Update Service

The NOC will provide anti-virus and anti-malware updates across all of its supported environments. Updates will be provided for a minimum of:

- McAfee Anti-Virus
- ClamAV Anti-Virus

Updates (anti-malware/anti-virus signatures updates as well as engine/software updates) will be accomplished on all supported isolated environments a minimum of weekly.

System log centralized collection, review, and archiving

The NOC will provide a centralized collection point for AFRl RDT&E system logs as well as a web based log review capability. The appropriate collected logs will be retained for a minimum of one year. Full logs or portions of the collected logs will be archived as defined by the NOC Program Manager.

Security Information and Event Management (SIEM)

The NOC will provide Security Information and Event Management (SIEM) or SIEM-like capabilities for system and network threat and risk assessment and continuous monitoring.

Assured Compliance Assessment Solution (ACAS) Scanning and Reporting

The NOC will provide a DISA Assured Compliance Assessment Solution (ACAS) scanning and reporting capability across all supported environments. Updates to the ACAS signatures and rules will be accomplished a minimum of monthly on all supported isolated environments.

A.2.3 Possible Future Expansion

There are a number of areas of possible future expansion of this effort.

A.2.3.1 Possible Future Environments or Task Areas

The following are task areas that could be added to this effort depending on available funding and approvals.

Network Troubleshooting

Providing a network engineer to do remote network troubleshooting at AFRL sites.

Centralized Site Firewall Administration and Monitoring

If the AFRL sites decided to, the NOC could take over administration, maintenance, and monitoring of the DREN border firewalls at AFRL DREN locations.

System Hosting and Management

It may be desirable to create an area within the Enterprise RDT&E IT data center to house AFRL Technology Directorate or project specific RDT&E servers. This would be a server hosting service.

Mobile Support

With more and more system and application access coming from mobile devices, additional provisions and support may need to be added to support access by these types of devices.

A.2.3.2 Possible Future Capabilities

Some future capabilities that could be added to the AFRL Enterprise RDT&E NOC depending on available funding and approvals are:

Centralized Server and or Workstation Backups

The capability for centralized backups for AFRL site RDT&E workstations and servers. This could be an on premise solution, a cloud based solution, or perhaps a hybrid solution.

Centralized Enterprise File Serving

The capability for large scale centralized file serving. Currently each site and organization within AFRL has their own file servers in the RDT&E environment. A centralized capability could be more labor and cost effective.

Hybrid On-Premis/Cloud RDT&E Data Archive

The capability for a long term data archive for data that needs to be stored for 20+ years but may not need to be accessed very often. If implemented, this is likely to be a hybrid on-premise/cloud based solution.

Software License Administration

The capability for centralized software license administration. Currently each site and organization within AFRL has their own license servers in the RDT&E environment. A centralized capability could be more labor and cost effective.

Cross Network Data Transfer Services

The capability to transfer data between network environments (Unclass DREN and Unclass Isolated) as well as from lower classification levels to higher levels (Unclassified to Collateral Secret network data transfers).

Automated Remote Network Monitoring and Testing

Implementing and managing remote sensors to monitor network performance and reliability or to automatically and regularly test connectivity to services or measure throughput between AFRL sites across the supported environments.

APPENDIX B: Federal, DoD, and Air Force IT and Cyber Security Policies and Instructions

The following list of Federal, DoD, and Air Force IT and Cyber Security policies are applicable to this PWS and the work being done under it. In the event that a policy is updated or replaced, the new or updated policies are also applicable to this PWS. The government will notify the contractor when there is a change in applicable IT policies that may affect the work being conducted under this PWS.

https://www.e-publishing.af.mil/

AFI 10-701	Operations Security (OPSEC)
AFI 61-201	Management of Scientific and Technical Information (STINFO)
AFI 16-1404	AF Information Security Program
AFI 16-1405	AF Personal Security Program
AFI 16-1406	AF Industrial Security Program
AFI 33-204	Information Assurance (IA) Awareness Program
AFI 33-208	Information Protection Operations
AFI 33-364	Records Disposition-Procedures and Responsibilities
AFMAN 17-1301	Computer Security (COMPUSEC)

Directives & Manuals:

https://www.esd.whs.mil/dd/

DOD Instruction 5200.08	Security of DOD Installations and Resources
DOD Instruction 8580.1	Information Assurance in the Defense Acquisition System
DoD Instruction 8510.01	Rick Management Framework (RMF) for DoD Information Technology
DoD Instruction 8500.01	Cybersecurity

DoD Instruction 5230.24	Distribution Statements on Technical Documents
DoD Regulation 5200.08	Physical Security Program
DoD 5105.21-M, Volume 1	Sensitive Compartmented Information (SCI) IT Administration
DoD 5105.21-M, Volume 2	SCI Physical, Visitor, Technical
DoD 5105.21-M, Volume 3	SCI Administration of Personnel Security, Industrial Security
DoD 5220.22-M	National Industrial Security Program Operating Manual (NISPOM)
DoD 8570.01-M	Information Assurance Workforce Improvement Program
DoD 5205.07	Special Access Program (SAP) Policy
DoD 5205.07, Volume 1	SAP General Procedures
DoD 5205.07, Volume 2	SAP Personnel Security
DoD 5205.07, Volume 3	SAP Physical Security
DoD 5205.07, Volume 4	SAP Marking
DoDD 8140.01	Cyberspace Workforce Management

https://www.federalregister.gov/documents/2016/07/28/2016-17872/revision-of-omb-circular-no-a-130-managing-information-as-a-strategic-resource

Office of Management and Budget Circular A-130	Managing Information as a Strategic Resource

APPENDIX C. Service Delivery Summary

The definition of violation, as referenced throughout the table below, is as follows: Violations are actions determined to be non-compliant with the established performance standards, to include, but not limited to, errors (including grammatical errors), omissions, or delayed deliveries.

Performance Requirement	Performance Standard	Acceptable Quality Level (AQL)	Incentive/Disincentive	Inspection Method
General – Applies to Nearly Everything	100% of documentation and services shall be completed and submitted IAW the requirements established within the requirement documents (PWS \ work definition \ task directive \ task assignment form, etc.) and shall be compliant with all applicable governing regulations, policies, directives and guidance. 100% of documentation and services shall be completed (including required updates) and submitted NLT the established date for completion/receipt as identified in the requirement documents.	No more than 6 violations per month.	CPARS assessment ratings.	Checklist and Customer Input

Performance Requirement	Performance Standard	Acceptable Quality Level (AQL)	Incentive/Disincentive	Inspection Method
Project Planning and Management	The contractor shall develop, document, and maintain project plans 100% compliant with federal governing regulations, policies, directives, guidance and industry practice. 100% of project plans shall include the identification of applicable responsibilities, timelines, deliverables, risks, milestones and other elements as required. 100% of plan schedules and activities shall be coordinated with all required participants. All issues impacting project schedules shall be communicated to government staff within one business day after determination of impact. 100% of project plans shall be updated weekly.	No more than 2 violations per month.	CPARS assessment ratings.	Checklist
Security Incident Notification and Resolution	100% of security incidents, Classified Information	No allowable violations per month.	CPARS assessment ratings.	Checklist and Customer Input

Performance Requirement	Performance Standard	Acceptable Quality Level (AQL)	Incentive/Disincentive	Inspection Method
	Incidents (CII), and lost or stolen equipment shall be reported within one hour of detection to the government program manager. 100% of violations of security agreement terms or deliberate actions to circumvent security controls shall be are addressed in accordance with Government direction.		Each additional violation beyond the AQL will result in a payment reduction of 2% up to the maximum reduction of 6%.	
RADIX Scanning	All environments and systems shall be scanned using RADIX quarterly and resulting compliance reports provided to the government.	No more than 1 violations per year.	CPARS assessment ratings.	Checklist
ACAS Vulnerability Scanning	All environments and systems shall be scanned using ACAS weekly and resulting vulnerability reports provided to the government.	No more than 4 violations per year.	CPARS assessment ratings.	Checklist
Network and System Vulnerability Remediation	All physical and virtual servers shall have all Air Force designated Category 1, critical, and high vulnerabilities corrected or	No more than 1 violation per month on critical vulnerabilities. No more	CPARS assessment ratings. Each additional violation beyond the AQL will result in a payment reduction of 1%	Checklist

Performance Requirement	Performance Standard	Acceptable Quality Level (AQL)	Incentive/Disincentive	Inspection Method
	mitigated within one week of detection and identification. Air Force designated Category 2, 3, and medium vulnerabilities shall also be corrected or mitigated within 30 days. Air Force designated low vulnerabilities shall be corrected or mitigated within 60 days. The contractor shall create POA&M entries for any vulnerability that cannot be corrected, to document mitigation measures.	than 3 violations of other vulnerability categories.	up to the maximum reduction of 5%.	
System Log Review	All aggregated system logs on all supported environments shall be reviewed a minimum of once a week.	No more than 1 violations per month.	CPARS assessment ratings.	Checklist
HelpDesk Availability	The HelpDesk shall be manned and responsive from 8am to 5pm Eastern Time, Monday through Friday excluding government holidays. The contractor is responsible for resource	No more than 2 violations per month.	CPARS assessment ratings. Each additional violation beyond the AQL will result in a payment reduction of 1% up to the maximum reduction of 5%.	Checklist

Performance Requirement	Performance Standard	Acceptable Quality Level (AQL)	Incentive/Disincentive	Inspection Method
	substitution/coverage when a coordinated absence is greater than five consecutive work days.			
HelpDesk Inquiry	The contractor shall provide an initial response to helpdesk queries within 4 business hours. Requests received at the end of the business day shall be responded to the morning of the next business day. Updates must be made to open category 1 tickets a minimum of every three days.	No more than 2 violations per month.	CPARS assessment ratings.	Checklist and Customer Input
Account Management	The contractor shall create individual user accounts within 1 business day of receiving the completed and approved request form. Bulk account creation requests shall be processed and created within 5 business days.	No more than 2 violations per month.	CPARS assessment ratings.	Checklist and Customer Input
User collaboration site request	The contractor shall create new project, working group, community of interest, etc. sites within 5 business days	No more than 1 violation per month.	CPARS assessment ratings.	Checklist and Customer Input

Performance Requirement	Performance Standard	Acceptable Quality Level (AQL)	Incentive/Disincentive	Inspection Method
	of receiving an ELSZ program manager approved, request.			
Linux Update Service Updates	All DREN Linux repository mirrors shall be updated automatically nightly. Mirrors of the DREN Linux and other software repositories shall be updated in all isolated environments monthly.	No more than 1 violation per quarter.	CPARS assessment ratings.	Checklist and Customer Input
Windows Update Service Updates	The Windows Update Service shall be updated with current patches in all isolated environments weekly.	No more than 1 violation per month.	CPARS assessment ratings.	Checklist and Customer Input
Anti Malware Update Service Updates	Anti Malware engine and signatures updates shall be performed in all isolated environments weekly, both server and client.	No more than 1 violation per month.	CPARS assessment ratings. Each additional violation beyond the AQL will result in a payment reduction of 1% up to the maximum reduction of 5%.	Checklist and Customer Input
Operating System and Application Updates	All operating systems and applications across all supported environments	No more than 1 violation per year.	CPARS assessment ratings.	Checklist

Performance Requirement	Performance Standard	Acceptable Quality Level (AQL)	Incentive/Disincentive	Inspection Method
	shall be updated a minimum of once a month.			
System and data backups	The contractor shall perform weekly back-ups (full back-up each weekend with incremental back-ups nightly) of user data and system images. The contractor shall deliver unclassified back-up media (portable USB hard drives, backup tapes, etc.) to the ELSZ program management team for off-site storage (outside of the WPAFB building 676 data center) on a quarterly basis.	No more than 1 violation per month.	CPARS assessment ratings. Each additional violation beyond the AQL will result in a payment reduction of 1% up to the maximum reduction of 5%.	Checklist
Device firmware updates	Every device in every environment shall be reviewed quarterly and firmware updated if new versions are available.	No more than 4 violations per year.	CPARS assessment ratings.	Checklist
RMF Package Reviews and Updates	The ISSM will review and update the RMF package, as appropriate, at least quarterly.	No more than 1 violation per year.	CPARS assessment ratings.	Checklist

Performance Requirement	Performance Standard	Acceptable Quality Level (AQL)	Incentive/Disincentive	Inspection Method
System and configuration change control documentation	All system and application configuration changes must be documented to include original setting, new setting, reason for change, approval, who made the change, and when in the designated documentation system.	No more than 2 violations per month.	CPARS assessment ratings.	Checklist
System configuration management	Once an automated configuration management tool is implemented, all changes shall be made through the tool unless otherwise approved by the government program manager.	No more than 2 violations per month.	CPARS assessment ratings.	Checklist
Monthly Status Report	100% complete with all required appendices. 100% accurate. Submitted no later than (NLT) 10th calendar day of month following the reporting period and submitted concurrent with the monthly invoice.	No violations per month.	CPARS assessment ratings.	Checklist

Performance Requirement	Performance Standard	Acceptable Quality Level (AQL)	Incentive/Disincentive	Inspection Method
Monthly Invoice	100% complete with all required supplemental information. 100% accurate. Submitted no later than (NLT) 10th calendar day of month following the reporting period and submitted concurrent with the monthly status report.	No violations per month.	CPARS assessment ratings.	Checklist
Mandatory Government Training Compliance	100% of the training (for all contractor personnel performing under the task order, including all CLINs) shall be completed and submitted NLT the established date for training completion as mandated by the Government.	No violations per month.	CPARS assessment ratings.	Checklist
Personnel Availability	100% contractor personnel availability during required daily core hours or specific CLIN required schedules (with the exception of coordinated absences). The contractor is responsible for resource substitution/coverage when	No violations per month.	CPARS assessment ratings.	Personnel Availability

Performance Requirement	Performance Standard	Acceptable Quality Level (AQL)	Incentive/Disincentive	Inspection Method
	a coordinated absence is greater than five consecutive work days.			
Personnel Retention	100% compliance with staffing requirements identified in PWS paragraph xxx	No violations per month. No more than 10% personnel turnover (on an individual basis, not positional basis) within an annual performance period.	CPARS assessment ratings.	Checklist and Customer Input

Anticipated Roles and Estimated Manning Levels

	Est. Contract Year 1		Est. Contract Year 2		Est. Contract Year 3		Est. Contract Year 4		Est. Contract Year 5	
Role	ELSZ	NOC	ELSZ	NOC	ELSZ	NOC	ELSZ	NOC	ELSZ	NOC
Senior System Administrator (Linux/Unix)	1	1^4	1	1^4	1	1^4	1	1^4	1	1^4
Senior System Administrator (MS Windows)	0	1^4	0	1^4	0	1^4	0	1^4	0	1^4
Mid Level System Administrator (mostly Linux/Unix, some Windows)	1	1^4	1	1^4	1	1^4	1	1^4	1	1^4
Network Engineer (Cisco, FortiNet, TACLANEs)	0	1^4	0	1^4	0	2^4	0	2^4	0	2^4
Enterprise Cyber Security Specialist	0	1^4	0	1^4	0	2^4	0	2^4	0	2^4

	Est. Contract Year 1		Est. Contract Year 2		Est. Contract Year 3		Est. Contract Year 4		Est. Contract Year 5	
Role	ELSZ	NOC	ELSZ	NOC	ELSZ	NOC	ELSZ	NOC	ELSZ	NOC
HelpDesk Specialist	1	0	1	1	1	1	1	1	1	1
Information System Security Manager (ISSM) for Enterprise RDT&E IT	0	1[4]	0	1[4]	0	1[4]	0	1[4]	0	1[4]
Technical/Team Manager	0	1[4]	0	1[4]	0	1[4]	0	1[4]	0	1[4]
Network enclave on-boarding specialist (remote site/RMF support)	0	1	0	1	0	1	0	1	0	1
Network Troubleshooter (remote site support)	0	0	0	1[4]	0	1[4]	0	1[4]	0	1[4]
Software Tester	0	1	0	1	0	1	0	1	0	1

	Est. Contract Year 1		Est. Contract Year 2		Est. Contract Year 3		Est. Contract Year 4		Est. Contract Year 5	
Role	ELSZ	NOC	ELSZ	NOC	ELSZ	NOC	ELSZ	NOC	ELSZ	NOC
User Trainer and Training Content Developer	1	0	1	0	1	0	1	0	1	0
Senior Programmer/Web Developer	1	0	1	1	1	1	1	1	1	1
TOTALS	5[1]	9[2]	5[1]	12[2]	5[1]	14[2]	5[1]	14[2]	5[1]	14[2]
	14		17		19		19		19	

1 AFRL Corporate Funded (ELSZ Core, FY17+)
2 AFRL Corporate Funded (RDT&E NOC, FY20+)
3 AFRL MS&A funded (FY18-FY19)
4 Top Secret security clearance required